(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 November 2001 (29.11.2001)

PCT

(10) International Publication Number
WO 01/90962 A1

(51) International Patent Classification[7]: G06F 17/60, 12/14, G07F 19/00

(21) International Application Number: PCT/AU01/00453

(22) International Filing Date: 19 April 2001 (19.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PQ 7029 20 April 2000 (20.04.2000) AU

(71) Applicant *(for all designated States except US)*: **GROSVENOR LEISURE INCORPORATED** [SC/SC]; 102 Aarti Chambers, Mont Fleuri, Victoria, Mahe (SC).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **TAYLOR, Barry, John** [AU/AU]; C/- Mr A Peterson, Level 2, 343 Little Collins St, Melbourne, VIC 3000 (AU).

(74) Agent: **PULLEN, Kevin, M**; P.O. Box 241, Landsborough, QLD 4550 (AU).

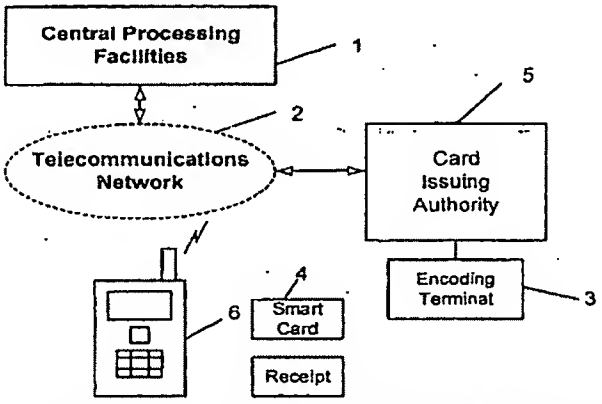
(81) Designated States *(notional)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SECURE BIOMETRIC IDENTIFICATION



(57) Abstract: A method and device/terminal are disclosed for the positive identification ofan individual which finds particular use for the secure purchasing of goods orservices over a visual medium such as television, the Internet and EFTPOSsystems. The terminal is a point-of-sale terminal (6) which includes akeyboard (7), a screen (8), a fingerprint reader (9), a smart card readerassembly (10) and a printhead assembly incorporated within the card readerassembly (10). The operating software of the terminal (6) includes code todecrypt encrypted information read from the smart card (4). An individualwishing to undertake a secure financial transaction first obtains a smart card(4) which incorporates encrypted biometric data and financial data of thatindividual. At the point of intended purchase, the card (4) is placed in thereader assembly (10) of the terminal (6). The account details and encryptedbiometric data are read by the terminal (6). The appropriate fingerprint of theindividual is then taken at the fingerprint reader (9) of the terminal (6) fromwhich the encryption key is determined. The encrypted fingerprint data readfrom the card (4) is then decrypted using the encryption key just determinedand the thus-decoded fingerprint data from the card (4) is compared with thefingerprint data obtained at the terminal (6). If the thus-read fingerprint data isidentical with that decoded from the card (4), identification is deemed positiveand the financial transaction proceeds.

WO 01/90962 A1

TITLE: SECURE BIOMETRIC LOOP

THIS INVENTION relates to the provision of a secure method for the positive identification of an individual, particularly, but not exclusively, as a means for the authentication of a purchase of goods or services or for cash withdrawals over a telecommunication medium. The invention finds particular, but not exclusive, use as a means for secure purchasing of goods or services over a visual medium such as television or other visual display medium or the Internet or as part of an EFTPOS system (electronic funds transfer at point of sale). However, the invention is not to be regarded as limited to such applications.

The advertising of goods and services over media such as television and the Internet is now commonplace. With television advertising, the public can often purchase the goods or services so-advertised over the telephone using a credit card facility. With the Internet now well known as an electronic medium and powerful communications tool the seamless system (World Wide Web) linking information on different computers, the general public can readily access the Internet for a wide variety of purposes, including to order numerous consumer goods and/or services online. Once again, payment for these goods and/or services is often by a credit card facility. Yet again, payment of goods at their point of sale by credit or debit cards (EFTPOS) is now common in the marketplace.

A significant disadvantage of telecommunication purchasing is that it does not provide positive identification of individuals which is important for preventing unauthorized access to bank account or credit card details by a person wishing to purchase goods or services fraudulently.

Possibly the most common method of positive identification before a sale is authorized over a telecommunication medium is the use of a code specific for

a particular account. These codes, often numeric but can be alphabetical or alphanumeric, are known as PIN numbers (Personal Identification Number) and are used in combination with the particular account number. However, as PIN and account numbers are not dependent on any cross-checking to ensure that they are being quoted over the telecommunication medium by the true proprietor of that PIN number and its associated credit card or bank account, this type of secure transaction is not too difficult to circumvent.

In particular, in current systems utilizing such a magnetic strip credit or debit card, both the user's account identification and PIN number are stored on the card. While this data is encoded, the card can be easily duplicated and then used fraudulently in at least two ways:

1. If the fraudulent user holds the card, a transaction can be completed, without a signature or PIN number, by several methods including over the telephone and the Internet using the card number, card name and expiry date.

2. If the fraudulent user knows the PIN number, then a substitute card can be used in ATM's, EFTPOS terminals, etc.

These fraudulent transactions create liability for both the issuing authority - which may be a bank building society or other financial institution - and the cardholder leading to subsequent disputes between the two parties.

Positive identification of an individual is also important for preventing unauthorized access to, or passage from, selected locations or facilities such as international destinations, bank vaults and other restricted areas which include secure buildings, jails, airport terminals, etc.

However, this positive identification of an individual can lead to delays for travellers crossing international borders as officials attempt to confirm the identity of the individual by, for example, manual interrogation, comparison of visual features with photographs in passports, or comparing names with lists of restricted individuals who may be banned from entering or leaving a particular country.

One prior art solution proposed for these particular problems is to adopt methodologies relying on a physical attribute of the individual. Such methodologies, commonly referred to as biometric techniques, include fingerprint analysis, thermograms and DNA analysis. These methodologies are considered less vulnerable to mistaken identity.

One such method includes comparing the biometric data on a card proffered by an individual to a previously created database of biometric data of authorized individuals. However, this system can still be foiled by individuals who have obtained a biometric card from its rightful owner. Alternatively, a fraudulent user of the card may partially duplicate the card, retaining any credit details but substituting his/her own biometric data for that of the rightful owner of the card. Further, the data obtained from the individual is usually compared to a vast remote databank of such information which is usually difficult and/or slow to locate and access.

The presently available methods to overcome the above discussed disadvantages can conveniently be summarized as possession of a passport, knowledge of a password, possession of a restricted article such as a pass key, and biometric techniques comparing data on a card by an individual to a remote databank of such information.

However, such security methods are readily circumvented and do not provide satisfactory methods for the positive and expedient identification of an individual.

It is thus a general object of the present invention to overcome, or at least ameliorate, one or more of the above problems and/or disadvantages.

According to a first aspect of the present invention, there is provided a method for the positive identification of an individual, said method including:

providing a unique description for said individual, said unique description including biometric data of said individual;

encrypting said unique description with an encryption key, said encryption key determined from said biometric data;

providing identification means adapted for carriage with said individual, said identification means containing said unique description;

providing a reading means to obtain verification biometric data from a person offering said identification means;

determining an encryption key from said verification biometric data;

using said encryption key from said verification biometric data to decrypt said biometric data included in said unique description; and

comparing said verification biometric data with said thus decrypted biometric data;

wherein identification of said person is deemed positive if said verification biometric data from said person is identical with said biometric data of said individual included in said unique description.

Preferably, said encryption key is determined from only a part of said biometric data.

Preferably, said biometric data is a fingerprint analysis.

Preferably, said identification means is a card of the type capable of holding information in a machine-readable form.

Optionally, after said reading means has obtained said verification biometric data from said person and said person has been initially positively identified, said verification biometric data is transmitted to a remote databank for further comparison with biometric data held in said databank.

In one embodiment of the present invention, said individual attends a point of issue for said identification means, such as a bank, where normal identification procedures for banking or credit card facilities must be met before said identification means is issued.

According to a second aspect of the present invention, there is provided a device for use in a method for the positive identification of an individual as hereinbefore described, said device including:

a facility to obtain said verification biometric data from a person offering said identification means;

reading means to read said identification means;

decoding means to obtain biometric data from said identification means; and

comparison means to compare said biometric data with said verification biometric data.

Preferably, said facility is a fingerprint reader.

Preferably, said reading means is a smart card reader assembly.

Preferably, said reading means is, or is incorporated as part of, a computer, mobile telephone, EFTPOS terminal, ATM, or similar terminal.

In those embodiments where said reading means is incorporated into a mobile telephone, said identification means is incorporated into the SIM card of the mobile telephone.

Optionally, said device will allow a maximum of three consecutive attempts to obtain said verification biometric data and compare with said biometric data included within said identification means. If positive identification does not occur within those three attempts, the identification is deemed negative.

In a third aspect of the present invention, there is provided a method for a secure transfer of data over a telecommunication medium, said method including:

providing a transmission means to transmit said data from a person desirous of undertaking a transaction to a party requiring to verify said data in order to validate said data before said transaction can be undertaken; and

providing a validation means to ensure that said person is authorized to undertake said transaction;

wherein said transaction is authorized upon positive identification of said person determined by the method for positive identification as hereinbefore described.

Preferably, said data is financial data of said person.

Preferably, said transmission means includes a terminal remote from said party whereby said person can supply said data to said party and which includes a cellular telephone or wireless data transmission link.

Thus, according to a fourth aspect of the present invention, there is provided a terminal for use in a method for a secure transfer of data as hereinbefore described, said terminal including:

transmission means to transmit identification details relevant to said person to said party; and

a facility for said person to provide verification biometric data of said person with said identification details.

Preferably, said transmission means further includes a credit or debit card slot assembly.

Preferably, said facility includes:

procuring means to obtain said verification biometric data from an individual offering said identification means;

reading means to read said identification means;

decoding means to obtain biometric data from said identification means;

comparison means to compare said biometric data with said verification biometric data; and

authentication means to authenticate said transfer of data.

Preferably, said procuring means is a fingerprint reader.

Preferably, said reading means is a smart card slot assembly wherein said smart card contains said biometric data.

More preferably, said facility further includes a printout means to produce a hard copy for recording details of said transfer of data.

In one embodiment of this aspect of the present invention, said printout means is a printer either integral with, or separate from, said facility.

In another embodiment of this aspect of the present invention, said printout means is located within said smart card slot assembly. A print head assembly, which may be of a mechanical, thermal, laser or inkjet type, prints a receipt when the receipt is entered (or withdrawn) from the slot assembly subsequent to the completion of the transfer of data and removal of the smart card from the slot assembly. A sensor of either optical or magnetic type detects the presence of the inserted blank receipt and activates the printing process.

Preferably, said receipt is a single, duplicate or triplicate receipt in the form of a "tear off pad".

More preferably, said receipt is a multiple copy receipt of comparable size to a credit or debit card.

Most preferably, said receipt is in triplicate.

A preferred embodiment of the present invention will now be described with reference to the accompanying drawings, wherein:

FIG. 1 is a diagrammatic simplistic representation of a terminal which incorporates the present invention for the positive identification of an individual wishing to undertake a financial transaction over that terminal;

FIG. 2a is a top plan view schematic representation of the terminal of the present invention; and

FIG. 2b is a top edge view schematic representation of the terminal of FIG. 2a.

With reference to FIG. 1, there is a central processing unit (1) connected to a cellular telecommunications network (2). A fingerprint reader (3) is connected to a smart card (4) issuing terminal (5) which can communicate with the network (2). It will be appreciated by those skilled in the art that each of these components are known and their interconnection possible by any suitable means known in the art. A transaction terminal (6), placed at a merchant's place of business, is also in communication with the network (2). As illustrated in FIGS. 2a & b, the terminal (6) includes a keyboard (7) to enter details of a transaction, a screen (8) to display the thus-entered details, a fingerprint

reader (9), a smart card reader assembly (10) and a printhead assembly (not illustrated) incorporated within the card reader assembly (10). The operating software of the terminal (6) includes code to decrypt encrypted information read from the smart card (4). Once again, it will be appreciated by those skilled in the art that each component of the terminal (6) is known and interconnection of the various components can be undertaken by known methods.

An individual wishing to undertake a secure financial transaction using a machine-readable card first obtains a card which incorporates encrypted biometric and financial data of that individual. This is achieved by presenting him- or herself to an institution such as a bank which issues machine-readable "smart" cards. As is usual when applying for a credit or debit card at such an institution, the individual must first provide positive identification which meets the requirements of the institution before proceeding. Once assigned a smart card, biometric data, in particular, fingerprint data, of the individual is taken at the institution using any suitable fingerprint reader known in the art. Although not essential, data can be taken from two fingerprints to minimize any subsequent false rejection that may occur when the present invention is in use at a merchant's place of business. The scanned image of the fingerprint(s), which is represented by a mathematical representation of the ridge pattern, is then compressed and encrypted using any appropriate encryption algorithm known in the art of financial transactions to ensure that it can only be read or compared by first decrypting the data. This encrypted biometric data and the financial details of the individual are stored in the memory of the smart card.

To undertake a secure purchase using this card (4), at the point of intended purchase, the card (4) is placed in the reader assembly (10) of the terminal (6) whereby the value of the transaction is enter by the merchant using the

keyboard (7). The value of the purchase is displayed on the visual display screen (8). The account details and encrypted biometric data are also read by the terminal (6). The appropriate fingerprint of the individual is then taken at the fingerprint reader (9) of the terminal (6) from which the encryption key is determined. The encrypted fingerprint data read from the card (4) is then decrypted using the encryption key just determined and the thus-decoded fingerprint data from the card (4) is compared with the fingerprint data obtained at the terminal (6); if the thus-read fingerprint data is identical with that decoded from the card (4), identification is deemed positive and the financial transaction proceeds. If the comparison is deemed negative, the customer represents the finger, or alternative finger if two such fingerprints have been stored on the card (4), for a second scan whereby the comparison process described above is repeated. Although this procedure could be repeated several times, in practice, it is expected that the terminal (6) will be set to allow only a maximum of three consecutive attempts to obtain the verification biometric data and compare with the biometric data included within the smart card (4). If validation does not occur within those three attempts, the identification is deemed negative.

Upon a positive transaction, a receipt is inserted in the reader/printer slot (10) and the details of the transaction are recorded on the receipt. Details of the transaction are also transmitted to the central processing facilities (1) for record purposes.

Although in no way limiting, this embodiment is particularly suitable for point of sale purchasing of goods or services in all markets. The terminal can be a self-contained stand-alone unit, or used in cooperation with a palmtop, laptop or desktop computer or any other unit which includes a visual display unit. Further, the terminal can utilise any convenient telecommunication network, and can be any combination of cellular, satellite, microwave or hard wire

telephone or other communication network although, preferably, the terminal will be a wireless communication device incorporating the functionality and convenience of a mobile cellular telephone.

Also, the secure transfer features of the present invention can be attached to existing ATM machines (Automatic Teller Machines) thus increasing the security of withdrawals therefrom.

By using the present invention, a number of advantages are obtainable including:

As verification of the identity of the person offering the identification means can be undertaken without accessing a remote database, this verification can be undertaken quickly and in significantly less time than the 20 to 30 seconds required by present means where a central database has to be accessed.

Fraudulent use of a credit or debit card can be eliminated. Although a partial duplicate of smart card data can be made keeping the credit data, replacing biometric data of the true owner of the card with that of the fraudulent user is insufficient to create a valid card as the encryption key is different being based on the original biometric data.

Thus the present invention, with its use of an encryption key based on biometric data of the person originally issued with a credit or debit card or other machine-readable identification means, prevents card fraud or other false identification with a high level of security, ease of use and application.

It will be appreciated that the above described embodiments are only exemplification of the various aspects of the present invention and that

modifications and alterations can be made thereto without departing from the inventive concept as defined in the following claims.

CLAIMS

1. A method for the positive identification of an individual, said method including:

providing a unique description for said individual, said unique description including biometric data of said individual;

encrypting said unique description with an encryption key, said encryption key determined from said biometric data;

providing identification means adapted for carriage with said individual, said identification means containing said unique description;

providing a reading means to obtain verification biometric data from a person offering said identification means;

determining an encryption key from said verification biometric data;

using said encryption key from said verification biometric data to decrypt said biometric data included in said unique description; and

comparing said verification biometric data with said thus decrypted biometric data;

wherein identification of said person is deemed positive if said verification biometric data from said person is identical with said

biometric data of said individual included in said unique description.

2. A method as defined in Claim 1, wherein said encryption key is determined from only a part of said biometric data.

3. A method as defined in Claim 1 or Claim 2, wherein said biometric data is a fingerprint analysis.

4. A method as defined in any one of Claims 1 to 3, wherein said identification means is a card of the type capable of holding information in a machine-readable form.

5. A method as defined in any one of Claims 1 to 4, wherein after said reading means has obtained said verification biometric data from said person and person has been initially positively identified, said verification biometric data is transmitted to a remote databank for further comparison with biometric data held in said databank.

6. A device for use in a method for the positive identification of an individual as defined in any one of Claims 1 to 5, said device including:

a facility to obtain said verification biometric data from a person offering said identification means;

reading means to read said identification means;

decoding means to obtain biometric data from said identification means; and

comparison means to compare said biometric data with said verification biometric data.

7. A device as defined in Claim 6, wherein said facility is a fingerprint reader.

8. A device as defined in Claim 6 or Claim 7, wherein said reading means is a smart card reader assembly.

9. A device as defined in any one of Claims 6 to 8, wherein said reading means is, or is incorporated as part of, a computer, mobile telephone, EFTPOS terminal, ATM, or similar terminal.

10. A device as defined in Claim 9 wherein said reading means is, or is incorporated as part of, a mobile telephone.

11. A device as defined in Claim 10, wherein said identification means is incorporated into the SIM card of said mobile telephone.

12. A method for a secure transfer of data over a telecommunication medium, said method including:

providing a transmission means to transmit said data from a person desirous of undertaking a transaction to a party requiring to verify said data in order to validate said data before said transaction can be undertaken; and

providing a validation means to ensure that said person is authorized to undertake said transaction;

wherein said transaction is authorized upon positive identification of said person determined by the method for positive identification as defined in any one of Claims 1 to 5.

13. A method as defined in Claim 12, wherein said data is financial data of said person.

14. A method as defined in Claim 12 or Claim 13, wherein said transmission means includes a terminal remote from said party whereby said person can supply said data to said party and which includes a cellular telephone or wireless data transmission link.

15. A terminal for use in a method for a secure transfer of data as defined in any one of Claims 12 to 14, said terminal including:

transmission means to transmit identification details relevant to said person to said party; and

a facility for said person to provide verification biometric data of said person with said identification details.

16. A terminal as defined in Claim 15, wherein said transmission means further includes a credit or debit card slot assembly.

17. A terminal as defined in Claim 15 or Clam 16, wherein said facility includes:

procuring means to obtain said verification biometric data from an individual offering said identification means;

reading means to read said identification means;

decoding means to obtain biometric data from said identification means;

comparison means to compare said biometric data with said verification biometric data; and

authentication means to authenticate said transfer of data.

18. A terminal as defined in Claim 17, wherein said procuring means is a fingerprint reader.

19. A terminal as defined in Claim 17 or Claim 18, wherein said reading means is a slot assembly for a smart card wherein said smart card contains said biometric data.

20. A terminal as defined in any one of Claims 15 to 19, wherein said facility further includes a printout means to produce a hard copy for recording details of said transfer of data.

21. A terminal as defined in Claim 20, wherein said printout means is a printer either integral with, or separate from, said facility.

22. A terminal as defined in Claim 20 or Claim 21, wherein said printout means is located within said slot assembly for said smart card.

23. A terminal as defined in Claim 22, wherein said printout means prints a receipt when said receipt is entered into said slot assembly subsequent

to the completion of the transfer of data and removal of said smart card from said slot assembly.

24. A terminal as defined in Claim 22, wherein said printout means prints a receipt when said receipt is removed from said slot assembly subsequent to the completion of the transfer of data and removal of said smart card from said slot assembly.

25. A terminal as defined in Claim 23 or Claim 24, wherein said receipt is a single, duplicate or triplicate receipt in the form of a "tear off" pad.

26. A terminal as defined in any one of Claims 23 to 25, wherein said receipt is of comparable size to a credit or debit card.

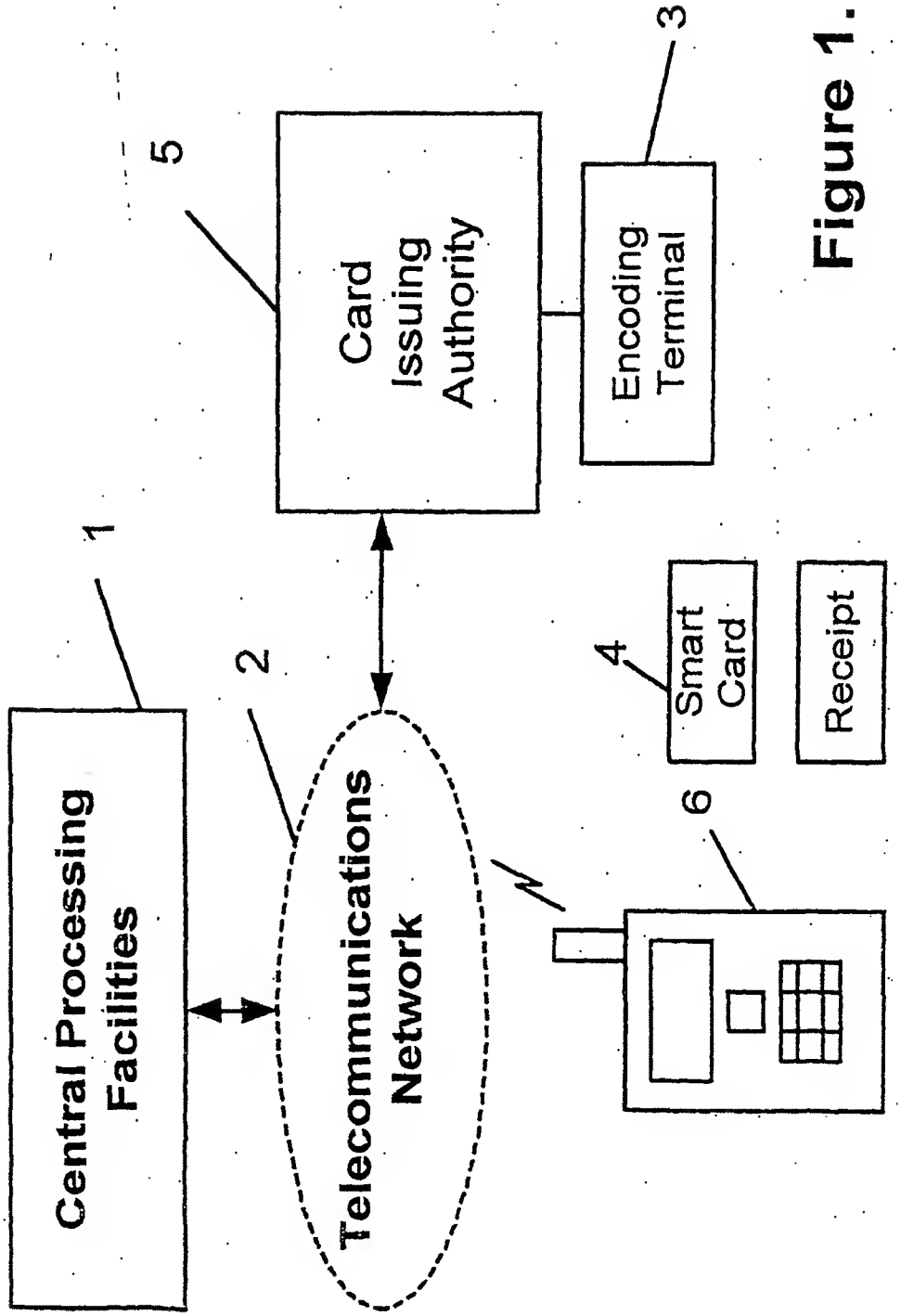

Central Processing Facilities
1
Telecommunications Network
2
Encoding Terminal
3
Smart Card
4
Card Issuing Authority
5
6
Receipt

Figure 1.

Figure 2.

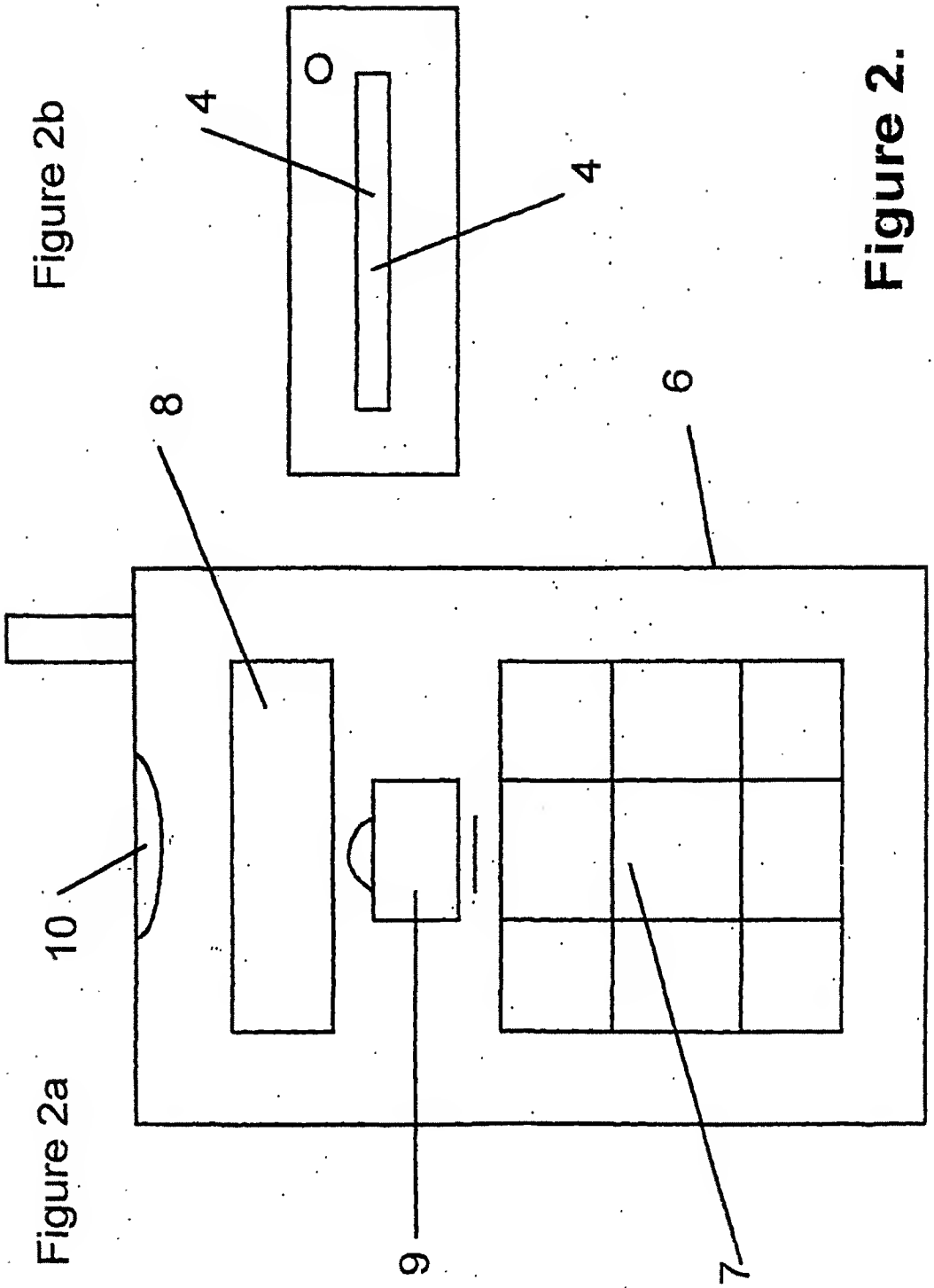


Figure 2b

Figure 2a

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU01/00453

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. [7]: G06F 17/60, 12/14; G07F 19/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC G06F, G06K, G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
AU:IPC AS ABOVE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPAT, USPTO

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5995630A, BORZA, 30 November 1999	1-26
Y	WO 9801820A, DYNAMIC DATA SYSTEMS PTY LTD, 15 January 1998	1-26
A	US 5712912A, TOMKO et al, 27 January 1998	

[X] Further documents are listed in the continuation of Box C [X] See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 June 2001	20 June 2001
Name and mailing address of the ISA/AU	Authorized officer
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	S KAUL Telephone No : (02) 6283 2182

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU01/00453

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6038666A, HSU et al, 14 March 2000	
A	EP 924655A, TRW INC, 23 June 1999	

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/AU01/00453

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report	Patent Family Member					
EP 924655	JP	11280317				
US 6038666	EP	924657	JP	11316818		
US 5712912	AU	47109/96	WO	9705578	US	5737420
	US	6002770	AU	33390/95	BR	9509002
	CA	2199034	CN	1157677	EP	780040
	US	5541994	WO	9608093	US	5832091
	US	5680460	AU	10895/97	WO	9725800
WO 9801820	AU	32489/97				
US 5995630	CA	2198993	EP	1012689	WO	9838567

END OF ANNEX